

⑥

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312221

(43)Date of publication of application : 25.10.2002

(51)Int.Cl.

G06F 12/00
G06F 12/14
G06K 19/073

(21)Application number : 2001-118507

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 17.04.2001

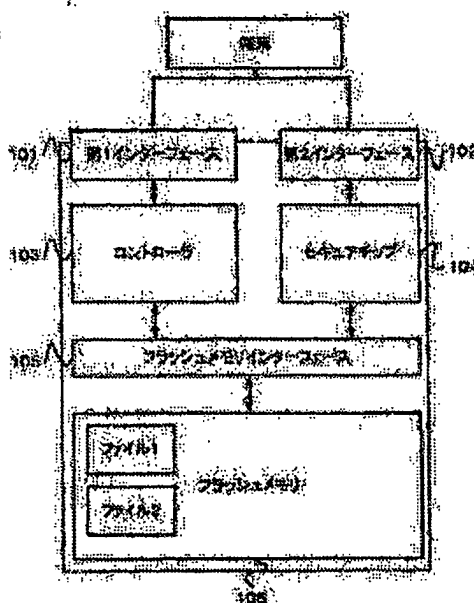
(72)Inventor : TAKAGI YOSHIHIKO
NAKANISHI YOSHIAKI
SASAKI OSAMU

(54) MEMORY DEVICE WITH ACCESS CONTROL FUNCTION AND FAILE ACCESS CONTROL PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a high protective property against wrong deletion and dishonest alteration of data in a memory device to write and read data.

SOLUTION: The memory device is provided with a controller 103 and a secure chip 104. A file, which is set so that its attribute cannot be changed when the secure chip 104 inputs 0 for a flag for determining whether the attribute of the access attribute peculiar to the file can be changed or not, cannot change the access attribute peculiar to the file by obtaining access through the controller 103. In a file, which is made through the controller 103, the flag for determining whether the attribute can be changed or not always becomes 1, making it possible to change the attribute freely. This constitution makes it possible to perform access control according to the degree of importance. In addition, in obtaining access through the secure chip 104, by applying access attribute according to conditions, a file to which access can be obtained only under a specific condition can be stored.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-312221
(P2002-312221A)

(43)公開日 平成14年10月25日 (2002. 10. 25)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 H 5 B 0 1 7
	5 4 2		5 4 2 J 5 B 0 3 5
12/14	3 1 0	12/14	3 1 0 K 5 B 0 8 2
G 0 6 K 19/073		G 0 6 K 19/00	P

審査請求 未請求 請求項の数14 O L (全 12 頁)

(21)出願番号 特願2001-118507(P2001-118507)

(22)出願日 平成13年4月17日 (2001. 4. 17)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 高木 佳彦

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 中西 良明

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100082692

弁理士 庵合 正博 (外1名)

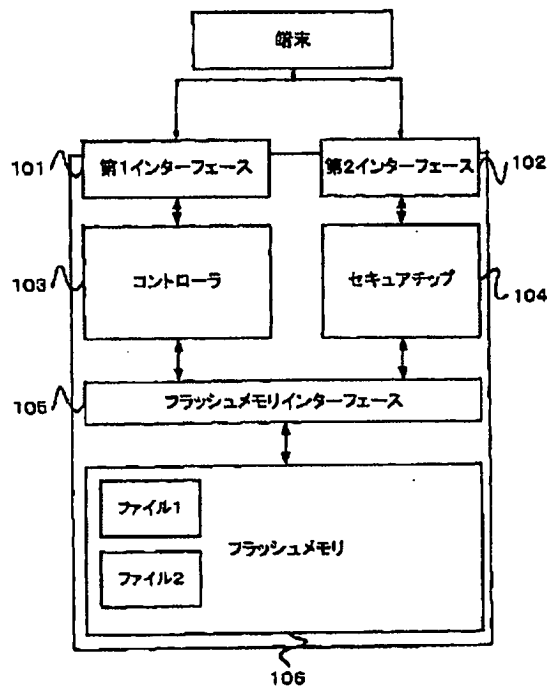
最終頁に続く

(54)【発明の名称】 アクセス制御機能付き記憶装置、及びファイル・アクセス制御プログラム

(57)【要約】

【課題】 データの書き込み、読み出しを行う記憶装置において、データの不正な削除、改ざんに対して高い防御性を実現することを目的とする。

【解決手段】 記憶装置にコントローラ103とセキュアチップ104を設け、セキュアチップ104がファイル固有のアクセス属性の属性変更可否フラグを0にすることによって属性変更不可に設定したファイルは、コントローラ103経由のアクセスではファイル固有のアクセス属性を変更できない。一方コントローラ103経由で作成したファイルは属性変更可否フラグは常に1となり、属性変更は自由である。これにより、ファイルの重要度に応じたアクセス制御を行うことができる。さらにセキュアチップ104経由のアクセスでは条件に応じたアクセス属性を適用することで、特定の条件下でのみアクセス可能なファイルを格納することができる。



【特許請求の範囲】

【請求項1】 ファイルと前記ファイルに固有のアクセス属性である第1の属性情報を格納する記憶手段と、前記第1の属性情報を参照して前記ファイルに対するアクセス制御を行う第1のアクセス制御手段と、前記記憶手段内部のファイルに対する条件に応じたアクセス属性を記述した第2の属性情報を格納する手段と、前記第2の属性情報を参照して前記ファイルに対するアクセス制御を行う第2のアクセス制御手段と、を備えたアクセス制御機能付き記憶装置。

【請求項2】 第2のアクセス制御手段が、前記第2のアクセス制御手段内部で実行するプログラムを記憶する手段と、前記プログラムの選択実行手段と、第2の属性情報を参照して前記プログラムによるファイルに対するアクセスの可否を判定する属性参照手段とを有し、前記第2の属性情報は、ファイルを一意に示す第1の参照情報と、前記ファイルに対してアクセスし得る1つ以上のプログラムをそれぞれ一意に示す第2の参照情報と、前記プログラムが前記ファイルに対してアクセスする際のアクセス属性と、を対応付けて記述されていることを特徴とする請求項1に記載のアクセス制御機能付き記憶装置。

【請求項3】 第2のアクセス制御手段が、第1の属性情報及び第2の属性情報に変更を施すことのできる属性変更手段を有することを特徴とする請求項2に記載のアクセス制御機能付き記憶装置。

【請求項4】 第1の属性情報又は／及び第2の属性情報として、属性変更手段のみが設定可能な、ファイルに対する属性情報の変更可否に関する情報を含むことを特徴とする請求項3に記載のアクセス制御機能付き記憶装置。

【請求項5】 第1の属性情報又は／及び第2の属性情報として、属性変更手段のみが設定可能な、ファイルに対する追加書き込み可否に関する情報を含むことを特徴とする請求項3に記載のアクセス制御機能付き記憶装置。

【請求項6】 第1の属性情報として、属性変更手段のみが設定可能な、ファイルに関する情報の取得可否に関する情報を含むことを特徴とする請求項3に記載のアクセス制御機能付き記憶装置。

【請求項7】 第1の属性情報又は／及び第2の属性情報として、属性変更手段のみが設定可能な、ファイルに対する削除可否に関する情報を含むことを特徴とする請求項3に記載のアクセス制御機能付き記憶装置。

【請求項8】 プログラムの実行により、記憶手段に格納されているファイルへのアクセスが生じ、第2の属性情報として、前記ファイルを示した第1の参

照情報と前記プログラムを示した第2の参照情報との対応付けを示した情報が記述されていない場合、属性参照手段は、第1の属性情報を参照して、前記ファイルへのアクセス可否の判定を行うことを特徴とする請求項2に記載のアクセス制御機能付き記憶装置。

【請求項9】 プログラムの実行により、記憶手段に格納されているファイルへのアクセスが生じ、前記アクセスが、第2の属性情報のアクセス属性の条件を満足していない場合、属性参照手段は、第1の属性情報を参照して、前記ファイルへのアクセス可否の判定を行うことを特徴とする請求項2に記載のアクセス制御機能付き記憶装置。

【請求項10】 記憶手段全体又は一部である領域に対するアクセス属性情報である第3の属性情報を格納する手段を備え、前記第3の属性情報として、前記領域に格納されたファイルに関する情報の取得可否に関する情報、又は／及び、前記領域内に属性変更可否に関する情報によって属性変更不可に設定されたファイルの存在有無を表す情報を含むことを特徴とする請求項4に記載のアクセス制御機能付き記憶装置。

【請求項11】 1つ以上のファイルの集まりであるファイル群に対するアクセス属性情報である第4の属性情報を格納する手段を備え、前記第4の属性情報として前記ファイル群に関する情報の取得可否に関する情報、又は／及び、前記ファイル群に対する属性変更可否に関する情報を含むことを特徴とする請求項4に記載のアクセス制御機能付き記憶装置。

【請求項12】 第1の属性情報又は／及び第2の属性情報として、その属性の適用範囲に関する情報を含み、前記適用範囲に関する情報に基づき、ファイルの一部に対するアクセス制御を行うことを特徴とする請求項1に記載のアクセス制御機能付き記憶装置。

【請求項13】 第2のアクセス制御手段が、暗号手段と復号手段とを備え、前記暗号手段は、記憶手段の全体もしくは一部、又は、記憶手段に格納された1つ以上のファイル、に暗号化を施して、前記暗号化の結果得られた暗号化データを前記記憶手段に格納し、

前記復号手段は、前記記憶手段に格納された前記暗号化データに復号化を施して、前記復号化の結果得られたデータを前記記憶手段に格納することを特徴とする請求項1に記載のアクセス制御機能付き記憶装置。

【請求項14】 ファイルへのアクセスを制御するためにコンピュータを、

ファイルと前記ファイルに固有のアクセス属性である第1の属性情報を格納する記憶手段、前記第1の属性情報を参照して前記ファイルに対するアクセス制御を行う第1のアクセス制御手段、

前記記憶手段内部の前記ファイルに対する条件に応じた

アクセス属性を記述した第2の属性情報を格納する手段、
前記第2の属性情報を参照して前記ファイルに対するアクセス制御を行う第2のアクセス制御手段、として機能させるためのファイル・アクセス制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、格納されたデータに対するアクセス及びデータを格納するアクセスに対して、適切なアクセス制御を実現するメモリカード等の記憶装置に関するものである。

【0002】

【従来の技術】従来のメモリカードは、端末を限定せずにメモリカードにデータを書き込んだり、読み出したりするものである。そのため、端末を限定してアクセス制御を行うことはできない。

【0003】一方、従来のICカードは、利用可能な端末や利用者を限定することでデータを保護するものである。そのため、限定されない端末による利用を想定していない。

【0004】

【発明が解決しようとする課題】以上のような従来のデータ記憶媒体にあっては、例えば銀行業務等の場合において、電子通帳としてメモリカードを利用する場合に、従来の通帳と同様に利用することを想定するならば、書き込みは、認証を行った正規の銀行端末のみが行うことができ、読み出しは、利用者が所有する端末等の一般の端末で、認証を行わずにできる必要がある。

【0005】また、利用者の端末を利用したメモリカードのアクセスにおいて、通帳データの改ざんや削除に対する防御が必要となる。

【0006】上記利用法を実現するためには、メモリカードに端末を限定しない場合と、認証を行って端末を限定する場合と、の両方に利用可能な機能を持たせることが必要である。また、端末を限定しない場合においても、読み出しのみ可能といった利用権限の限定を行う必要がある。

【0007】本発明は、上記従来の要請に鑑みてなされたもので、上記のようなアクセス制御をメモリカード自体に行わせることによって、不正なファイルの削除や改ざんを防止することを目的とする。

【0008】

【課題を解決するための手段】上記課題を解決するために、本発明は、第1に、ファイル固有のアクセス属性である第1の属性情報とは別に、第2のアクセス制御手段が、前記第2のアクセス制御手段内部のプログラムによるファイルへのアクセスを制御する際に参照する第2の属性情報属性情報を持つアクセス制御機能つき記憶装置である。

【0009】これにより、第2のアクセス制御手段内の

プログラムに対して、ファイル固有のアクセス属性（第1の属性情報）のみによる固定的・画一的・一括/包括的なアクセス制御とは異なる、特別な権限を与え、動的で多様なファイル・アクセス制御を実現することができる。

【0010】本発明は、第2に、第1の属性情報又は/及び第2のアクセス属性情報として、第2のアクセス制御手段内の属性変更手段のみが設定可能な、ファイルの属性変更可否フラグ、ファイル情報の取得可否フラグ、追加書き込み可否フラグを備える。上記3種の属性フラグは、第1のアクセス制御手段経由では設定又は変更ができない。その他のフラグに関しても、属性変更可否フラグによって変更不可に設定されていれば、第1のアクセス制御手段経由での変更ができない。

【0011】これにより、第2のアクセス制御手段経由で作成した重要なファイルに対する第1のアクセス制御手段経由でのアクセスを制限することができる。

【0012】一方、第1のアクセス制御手段経由で作成したファイルのアクセス属性は、属性変更可否フラグ、情報取得可否フラグ、追加書き込み可否フラグを除いて、第1のアクセス制御手段経由で自由に変更することができる。

【0013】本発明は、第3に、記憶手段の全体または一部に対して設定するアクセス属性情報と、記憶手段内部に属性変更不可に設定されたファイルの存在有無を表すフラグを備える。

【0014】これにより、第1のアクセス制御手段経由での記憶手段に対するアクセスを制限することができ、第2アクセス制御手段経由でのみ利用可能な状態にすることができる。また、属性変更不可であるファイルが存在するときに、記憶手段全体に対する処理を拒否することで、属性変更不可であるファイルを守ることができる。

【0015】本発明は、第4に、第1の属性情報が、属性適用範囲も同時に持ち、ファイルの一部に対するアクセス制御を行う。

【0016】これにより、条件によって、アクセス可能な範囲を第2アクセス制御手段によって変化させることができる。

【0017】

【発明の実施の形態】以下、本発明の実施の形態について、図1から図12を用いて説明する。なお、本発明はこれら実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲において種々なる態様で実施し得る。

【0018】図1は、本実施の形態の構成図である。図1において、101及び102は、端末と通信を行うインターフェースである。103は、端末が第1インターフェースを経由してフラッシュメモリにアクセスする場合に、ファイルシステム全体に対するアクセス属性及び

ファイルに付加されたアクセス属性を用いてアクセス制御を行うコントローラである。コントローラ103は、端末からのアクセス要求があった時に、ファイルシステムのアクセス属性及び対象ファイルのアクセス属性を参照し、アクセス要求がアクセス属性を満足していれば、アクセスを許可する。満足していなければアクセスを拒否する。ここでいう「アクセス」とは、ファイルに対する読み出し、書き込み、ファイルの情報取得、ファイルのアクセス属性変更であり、またそれ以外に考えられるすべてのファイルに対する操作である。

【0019】104は、端末が第2インターフェースを経由してフラッシュメモリにアクセスする場合に、端末との間で認証を行い、認証結果に基づいてアクセス制御を行うセキュアチップである。本実施の形態では、セキュアチップ104は、内部に1つ以上のアプリケーションを保持し、認証状態によって起動されるアプリケーションが異なる。例えば、電子通帳ファイルに記帳を行うアプリケーションは、銀行端末が正規認証を行った場合のみ起動することができる。銀行端末でない場合、通帳記帳アプリケーションが起動されることはない。105はコントローラおよびセキュアチップからフラッシュメモリにアクセスするためのフラッシュインターフェース、106はフラッシュメモリである。

【0020】コントローラ103の内部について図7を用いて説明する。コントローラ103は、内部に属性参照手段701とデータ通信路702を持つ。端末からあるファイルへのアクセス要求があると、属性参照手段701が対象ファイルのアクセス属性をチェックし、アクセス要求がアクセス属性を満足しているか判断する。満足していればデータ通信路702の利用が可能となり、アクセス要求を処理する。満足していなければ拒否する。

【0021】セキュアチップ104の内部について図6を用いて説明する。セキュアチップ104は、認証手段601、アプリケーション群602、属性参照手段603、アプリケーションアクセス属性情報（属性テーブル）604、属性変更手段605を持つ。認証を行うための必要な情報を秘密に保持するために、セキュアチップ104は耐タンパとなっており、認証機能には、署名検証、乱数生成や暗復号化等の演算機能を含む。アプリケーションアクセス属性情報604は、起動されたアプリケーションによって、ファイルへのアクセス権限を変化させるためのものであり、ファイルに対応したアクセス権限を保持するアプリケーションと、そのアクセス属性が登録されている。第1インターフェース経由のアクセスよりも高い権限を与えるためのものである。アプリケーションアクセス属性情報604は、属性参照機能603によって参照され、属性変更機能605によって変更される。

【0022】以下、図2を用いて、ファイルシステム及

びファイルに付加されたアクセス属性について説明する。図2は、フラッシュメモリ上のファイルシステムの構成図の一例であり、201は、コントローラ経由でのアクセスに適用されるファイルシステム全体に対するアクセス属性の設定であり、Rは読み出し属性、Wは書き込み属性、Vはファイル情報取得属性（ファイル情報については後述）、Eはアクセス属性変更不可データの有無を表す。R、W、Vについては、0ならば不可、1ならば可を意味する。Eについては、0ならばアクセス属性変更不可データは存在せず、1ならば存在することを意味する。

【0023】202は、コントローラ経由でのアクセスに適用されるファイルシステム内のファイル固有のアクセス属性であり、R、W、Vについてはファイルシステム全体のアクセス属性と同様なので説明を省略する。Aは追記属性を意味する。Cについては、コントローラ経由によるアクセス属性変更可否を表す。1ならば変更可であり、0ならば変更不可を意味する。

【0024】ファイル情報とは、ファイルの存在、ファイル名、ファイルサイズ、作成日時、アクセス属性であり、またそれ以外に考えられる全てのファイルに関する情報である。ファイル固有のアクセス属性202においてVが0に設定されていると、コントローラ経由での対象ファイルに関する情報の取得が拒否される。また、ファイル一貫取得の要求に対してもVが0に設定されているファイルは表示されない。

【0025】ファイルシステム全体のアクセス属性201においてVが0に設定されていると、ファイルシステム全体に対する情報の取得ができないので、結果として、コントローラ経由でのアクセスは全て拒否される。例えば、ファイルシステム全体のアクセス属性201において、RWVE=1111、ファイル固有のアクセス属性202においてRWACV=10001に設定されているファイルの場合、フラッシュメモリ全体のアクセス属性がV=1であるので、コントローラ経由で、ファイルに関する情報を取得することができる。また、R=1であるので、ファイルの内容を読み出すことが出来る。しかしコントローラ経由での書き込み要求に関しては、W=0であるので、コントローラ103によって拒否される。もしRWACV=10101のようにW=0つまり書き込み禁止設定であってもA=1ならば、該当ファイルに対して、追記のみ可能である。

【0026】また、アクセス属性の変更要求、例えばRWACV=10001から11001への変更要求を行ったとしても、C=0より、コントローラ経由によるアクセス属性の変更は不可であるので、拒否される。C=0であるファイルは、コントローラ経由によるファイルのアクセス属性変更が拒否される。また、ファイル名の変更、ファイルの削除を行うことが出来ない。現在の属性情報が対応するファイルの名称変更や属性情報自体の

消去は、属性情報変更とみなすからである。Cの変更が可能なのは、セキュアチップによる認証で、属性変更権限があるとみなされたアプリケーションによるアクセスのみであり、コントローラを経由したアクセスでは変更できない。

【0027】別の例として、ファイルシステム全体のアクセス属性201において、RWVE=1111、ファイル固有のアクセス属性202においてRWACV=10111の場合、W=0であるので、コントローラ経由での書きこみ要求に対しては、コントローラによって拒否されるが、C=1よりアクセス属性の変更を行うことができるので、W=1に変更することで、書き込みが可能となる。これによって、既存のメモ리카ードのように認証を介さない利用法も可能である。ファイルシステム全体のアクセス属性201に含まれるアクセス属性変更不可データの有無を表すEが1である場合は、ファイルシステム全体に対する処理であるフォーマット等のコマンドを拒否することで、属性変更不可データを守ることができる（なお、ファイル情報のうち、ファイル名、ファイルサイズ等の情報の格納方法については、ここでは省略する）。

【0028】以下、図3を用いて、アプリケーションアクセス属性情報604（300）について説明する。図3は、セキュアチップ内部のアプリケーションアクセス属性情報の一例であり、301はフラッシュメモリ内のファイル1を表すファイル番号、302は、セキュアチップ内部のアプリケーション1を表すアプリケーション番号、303は、アプリケーション1がファイル1にアクセスする場合の、アクセス属性を表す。アクセス属性303の各項目RWACについては、ファイル固有のアクセス属性202で説明した項目と意味が同じであるので、説明を省略する。

【0029】なお、アプリケーションアクセス属性は、1つのファイルに対して1つのアプリケーションのみを対応づけてもよいし、複数のアプリケーションを対応付けてもよい。その際、1つのファイルに対応したアプリケーションごとに異なるアクセス属性を設定してもよい。以下、端末からのフラッシュメモリへのアクセスについて説明する。図4は、コントローラを経由したフラッシュメモリへのアクセス処理の流れを示すフローチャートであり、図5はセキュアチップを経由したフラッシュメモリへのアクセス処理の流れを示すフローチャートである。図1乃至3とあわせてその流れを説明する。

【0030】まずコントローラ経由のアクセスについては、端末にカードが挿入され（ステップ401）、端末は第1インターフェース101に対して、アクセス要求を行う（ステップ402）。コントローラ103内部の属性参照機能701は、まずフラッシュメモリ全体のアクセス属性201を参照し（ステップ403）、端末の要求と比較して（ステップ404）、アクセス属性を満

足していなければ、コントローラ103がアクセス拒否を端末に伝える（ステップ405）。

【0031】アクセス属性を満足している場合は、対象ファイルが存在している場合、属性参照機能701が対象ファイル固有のアクセス属性202を参照し（ステップ406）、端末の要求と比較する（ステップ407）。その後、アクセス属性を満足していなければ、コントローラ103が、端末にアクセス拒否を伝える（ステップ408）。一方、アクセス属性を満足していれば要求を処理する（ステップ409）。対象ファイルが存在していない場合は、アクセス要求がファイルの新規作成以外の場合はエラーを返し、ファイルの新規作成ならば処理（ファイル新規作成）を行う。

【0032】次にセキュアチップ102経由のアクセスについては、端末にカードが挿入され（ステップ501）、端末とセキュアチップ104の間で認証を行う（ステップ502）。認証が完了すると、セキュアチップ104内部で認証結果に応じてアプリケーション群602の中から選択されたアプリケーションが起動される（ステップ503）。アプリケーションがファイルにアクセスを試みた時に（ステップ504）、ファイルが存在すれば、セキュアチップ104内部の属性参照機能603は、アプリケーションアクセス属性情報604を参照し（ステップ505）、該当ファイルにそのアプリケーションのアクセス属性が登録されているかどうかを調べる。そして、該当ファイルにそのアプリケーションのアクセス属性が登録されていれば、アプリケーションによるアクセスが、そのアクセス属性を満足しているかどうかを調べ（ステップ506）、アクセス属性を満足していれば、アプリケーションによるファイルへのアクセスを許可する（ステップ508）。

【0033】アプリケーションアクセス属性情報604にアクセス属性が登録されていなかった場合、もしくは、登録されていたが、アクセス属性を満足しなかった場合は、フラッシュメモリ内部の対象ファイルが持つ、ファイル固有アクセス属性を参照し、これに従ってアクセスの可否を判定する（ステップ507）。

【0034】ファイルが存在しなかった場合、アクセス要求が、ファイルの新規作成だった場合は、処理（ファイル新規作成）を行い、アプリケーションアクセス属性情報及びファイル固有アクセス属性は、ファイルを作成したアプリケーションによって指定され、属性変更機能605が設定する。

【0035】ここで、属性参照手段によるアクセス可否判定のパターンをまとめると次のようになる。つまり、

（1）第1の参照情報と第2の参照情報との対応付けが記述されていない場合と、（2）アクセス属性を満たさない場合（第1の参照情報と第2の参照情報との対応付けが記述されていてもアクセス属性が条件を満足しない場合）と、があり、（1）は、具体的には、プログラム

Aの実行によりファイルBへのアクセスが必要となった時に、(1-1)第1の参照情報として「ファイルB」の記述がない場合と、(1-2)第2の参照情報として「プログラムA」の記述がない場合と、(1-3)それぞれに記述があっても、それらが対応付けされていない場合と、があり、そのような場合、属性参照手段は、第1の属性情報を参照して、ファイルBへのアクセス制御を行う。

【0036】電子通帳への書き込みや、電子チケットの新規作成、削除という処理を行うことができるのは、認証を経た銀行端末や、チケット販売端末といった特定の端末である必要がある。しかし、電子通帳、電子チケットの閲覧、表示を行う時には、認証によって端末を限定しない方が、処理時間や利用者の入力手間を考えると、便利である場合がある。

【0037】本発明では、認証機能を持たない端末または認証を行っていない端末でも、ファイルに読み出し可能属性が与えられていれば、読むことができる。同時に、書き込み不可設定及びアクセス属性変更不可設定を行えば、認証機能を持たない端末から重要なファイルを変更される恐れがなく、安全かつ適切なセキュリティレベルを設定できるという効果がある。また、ファイルシステム全体のアクセス属性を変更できるセキュアチップ内のアプリケーションを利用すれば、認証を行った時のみファイルシステムを参照することが出来る、という機能を追加できる。

【0038】これにより、メモリカードを郵送する場合にあらかじめコントローラ経由によるファイルシステムへのアクセスを全て禁止しておけば、もしメモリカード自体を盗まれたとしても第三者にファイルを読まれることを防止できる。解除する時は、セキュアチップによる認証を行い、セキュアチップ内のアクセス属性変更用アプリケーションを利用すれば、解除することが出来る。

【0039】また、メモリカード内の情報を他人に見せたいが、変更、書き込み、削除といった処理を一切されたくない場合は、ファイルシステム全体のアクセス属性201において、RとVを1に設定し、Wを0に設定すれば、セキュアチップによる認証を行ってファイルシステムのアクセス属性を変更しない限り、読み出し専用メモリカードとなる。

【0040】さらに、図9のように、属性変更手段605によるコントローラ経由によるファイルシステムへのアクセスの禁止と同時に、暗号化手段901を用いてセキュアチップのみが秘密に保持する暗号鍵902によってファイルシステム内のファイルに暗号化を施すことによって、例えばメモリカードを分解してフラッシュメモリの内容を特殊な方法で直接読まれたとしても、容易には内容を読み出せないようにすることができる。

【0041】解除する時は、図10のように、属性変更手段605によるファイルシステムへのアクセスの許可と同時に、復号化手段1001を用いてセキュアチップ

のみが秘密に保持する復号鍵1002で暗号化データを復号化してファイルを復元する。この暗復号処理の実行を、ファイルシステム全体のアクセス属性変更権限の持つアプリケーションのみに限定しておけば、認証を伴わずに容易にフラッシュメモリ内のデータを読み出すことは困難となる。

【0042】なお、ファイルは、フラッシュメモリのアドレス直接指定による特定範囲であってもよい。また、ファイル固有のアクセス属性は、ファイルの一部に対するアクセス属性であってもよい。その場合、アクセス属性を設定する範囲を表すための情報をアクセス属性に含める。例えば、図8のように、ファイル先頭からの位置を表すsと、アクセス属性を設定するサイズeをアクセス属性に含めるといった具合である。また、例えば、格納データとして音楽ファイルを扱う場合に、料金未納時は音楽ファイルの先頭一部のみ読み出し可能に設定し、料金を支払うと、セキュアチップによって音楽ファイル全体を読み出し可能に設定するなどにより、視聴機能を実現できる。

【0043】また、アプリケーションは、ハードウェア(のみ)で構成された回路でもよい。また、ファイル固有の属性情報または、アプリケーションアクセス属性情報として、ファイルの削除の可否を表すフラグを属性変更可否フラグとは別に独立して持ってもよい。

【0044】また、メモリカードの構成は、図11のようにひとつのインターフェースを介して端末と通信し、セキュアチップに対する要求はコントローラを経由してセキュアチップに送信される構成でもよい。

【0045】また、メモリカードの構成は、図12のようにひとつのインターフェースを介して端末と通信し、通信内容によってコントローラとセキュアチップにデータが振り分けられる構成でもよい。

【0046】また、アプリケーションアクセス属性情報は、セキュアチップによってのみアクセス可能であれば、セキュアチップの外に設置してもよい。

【0047】また、端末によるフラッシュメモリへのアクセスは、コントローラ及びセキュアチップとの通信路とは別に、データ転送用の通信路を持ち、コントローラ及びセキュアチップによって、そのデータ通信路を制御してもよい。

【0048】また、本実施の形態におけるフラッシュメモリは、コントローラおよびセキュアチップによって制御可能であり、かつコントローラおよびセキュアチップを経由しなければアクセスが出来ないその他の記録媒体でもよい。

【0049】また、アクセス属性について、VとCの2つを、両者ともに0ならば、ファイル情報取得不可、Vのみ0であれば従来のフラッシュメモリにおける隠しファイル、Cのみ0であればアクセス属性変更不可、両者のみ1であれば、ファイル情報取得及びアクセス属性変

更に関して制限なし、というように相関させてもよい。

【0050】

【発明の効果】以上説明したように、本発明によれば、セキュアチップによって作成されたファイルのうち、アクセス属性変更を不可に設定したファイルは、コントローラ経由のアクセスでは、属性を参照するのみで変更することが出来ない。しかし、セキュアチップによって端末を認証し、正規のアクセス権限を持つアプリケーションによってのみ属性を変更することができる。これにより、従来のメモリカードでは行うことができなかった、メモリカード自身によるアクセス制御が可能になるという効果がある。

【0051】また、コントローラ経由では見られたくない重要なファイルのファイル情報取得属性を、セキュアチップによって不可に設定することで、コントローラ経由ではそのファイルの存在自体を知ることができなくなり、ファイルに対する不正の機会を減らすことが出来る。一方、コントローラを経由して作成されたファイルに関しては、アクセス属性は自由に設定することができ、従来のメモリカードと同じアクセス属性の設定も可能であるという効果がある。

【0052】また、ファイルシステム全体のアクセス属性を変更して、コントローラからのアクセスを完全に禁止することで、メモリカードを輸送するときや他人に預けるときに、第三者によるフラッシュメモリへのアクセスを禁止することや、読み出し専用を設定できるという効果がある。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるメモリカード構成図

【図2】本発明の実施の形態におけるファイルに固有のアクセス属性情報の図

【図3】本発明の実施の形態におけるセキュアチップ内部のアプリケーション別アクセス属性テーブルの図

【図4】本発明の実施の形態におけるコントローラ経由による端末からのアクセスのフローチャート

【図5】本発明の実施の形態におけるセキュアチップ経由による端末からのアクセスのフローチャート

【図6】本発明の実施の形態におけるセキュアチップ内部の構成図

【図7】本発明の実施の形態におけるコントローラ内部の構成図

【図8】本発明の実施の形態におけるファイルの一部に適用されるアクセス属性情報の図

【図9】本発明の実施の形態における暗号化機能をもったセキュアチップ内部の構成図

【図10】本発明の実施の形態における復号化機能を持ったセキュアチップ内部の構成図

【図11】本発明の実施の形態におけるインターフェースが1つであり、端末のセキュアチップとの通信はコントローラ経由で行うメモリカード構成図

【図12】本発明の実施の形態におけるインターフェースが1つであり、通信内容によってコントローラとセキュアチップにデータが振り分けられるメモリカード構成図

【符号の説明】

101 第1インターフェース

102 第2インターフェース

103、1103、1203 コントローラ

104、1104、1204 セキュアチップ

105 フラッシュメモリインターフェース

106 フラッシュメモリ

201 ファイルシステム全体のアクセス属性

202、801 ファイルに固有のアクセス属性

300 アクセス属性テーブル

301 ファイル番号

302 アプリケーション番号

303 アプリケーションに対応したアクセス属性

601 認証手段

30 602 アプリケーション群

603、701 属性参照手段

604 アプリケーション別アクセス属性テーブル

605 属性変更手段

606、702 データ通信路

901 暗号化手段

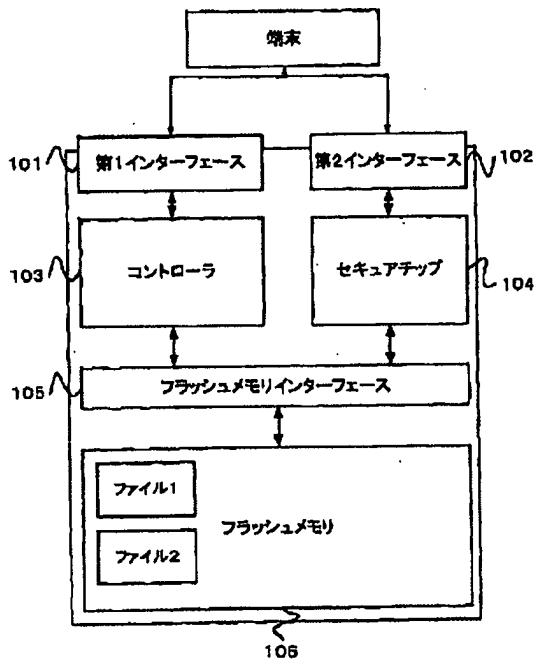
902 暗号鍵

1001 復号化手段

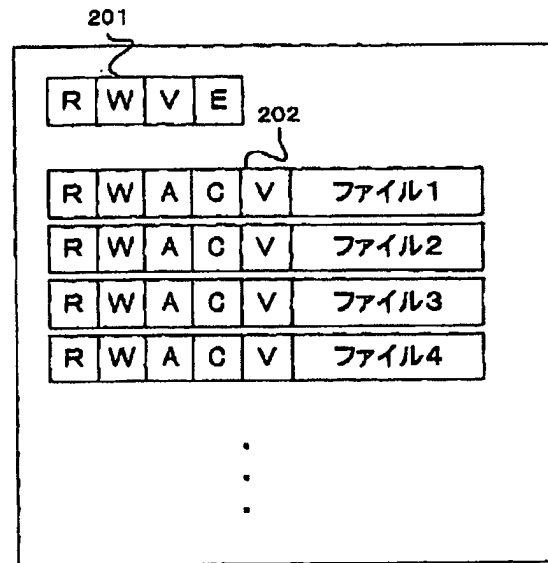
1002 復号鍵

1101、1201 インターフェース

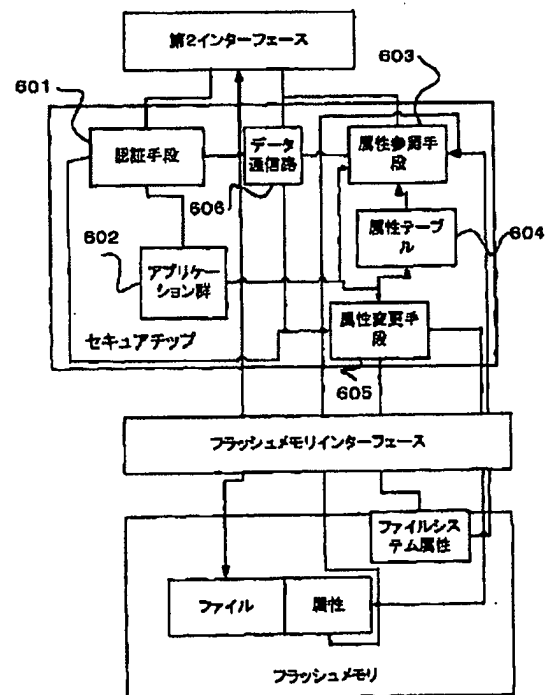
【図1】



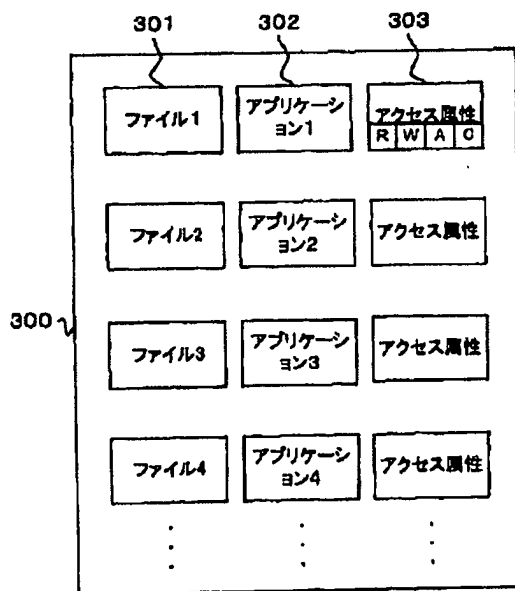
【図2】



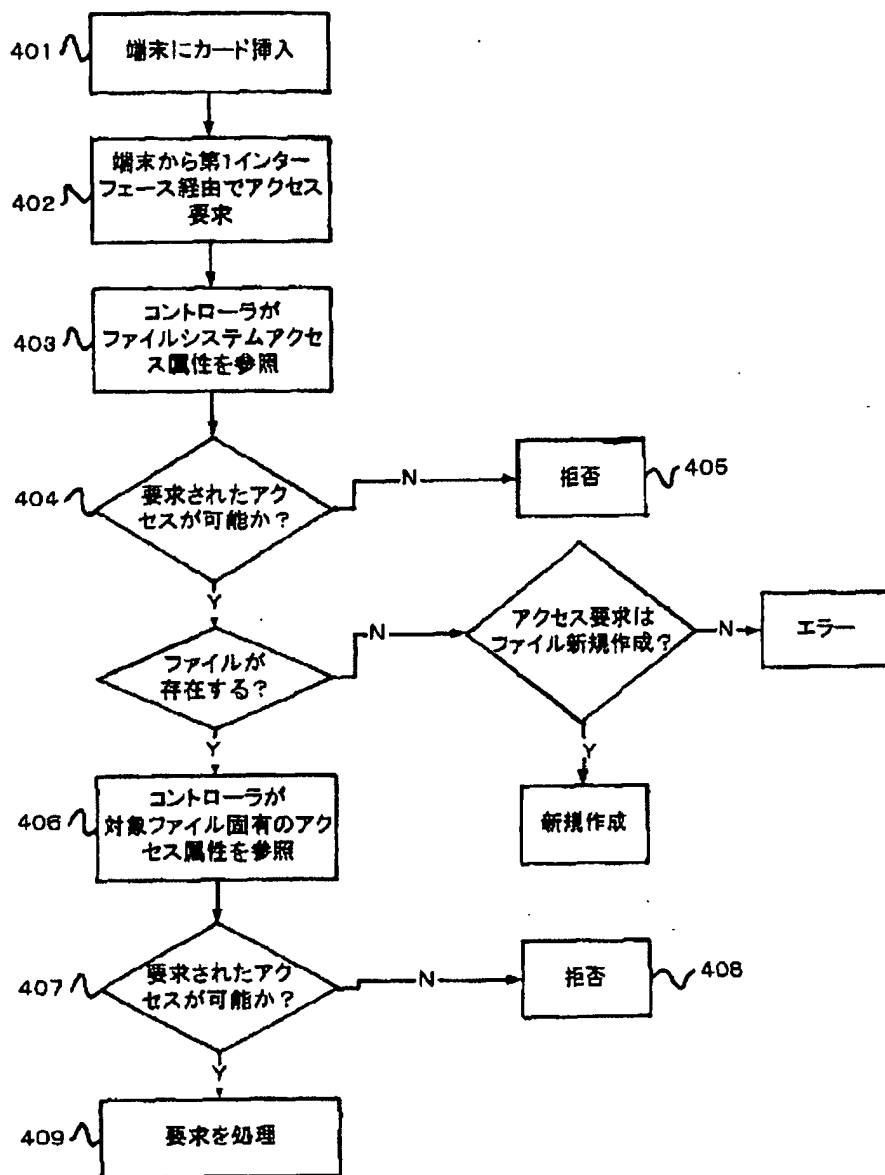
【図6】



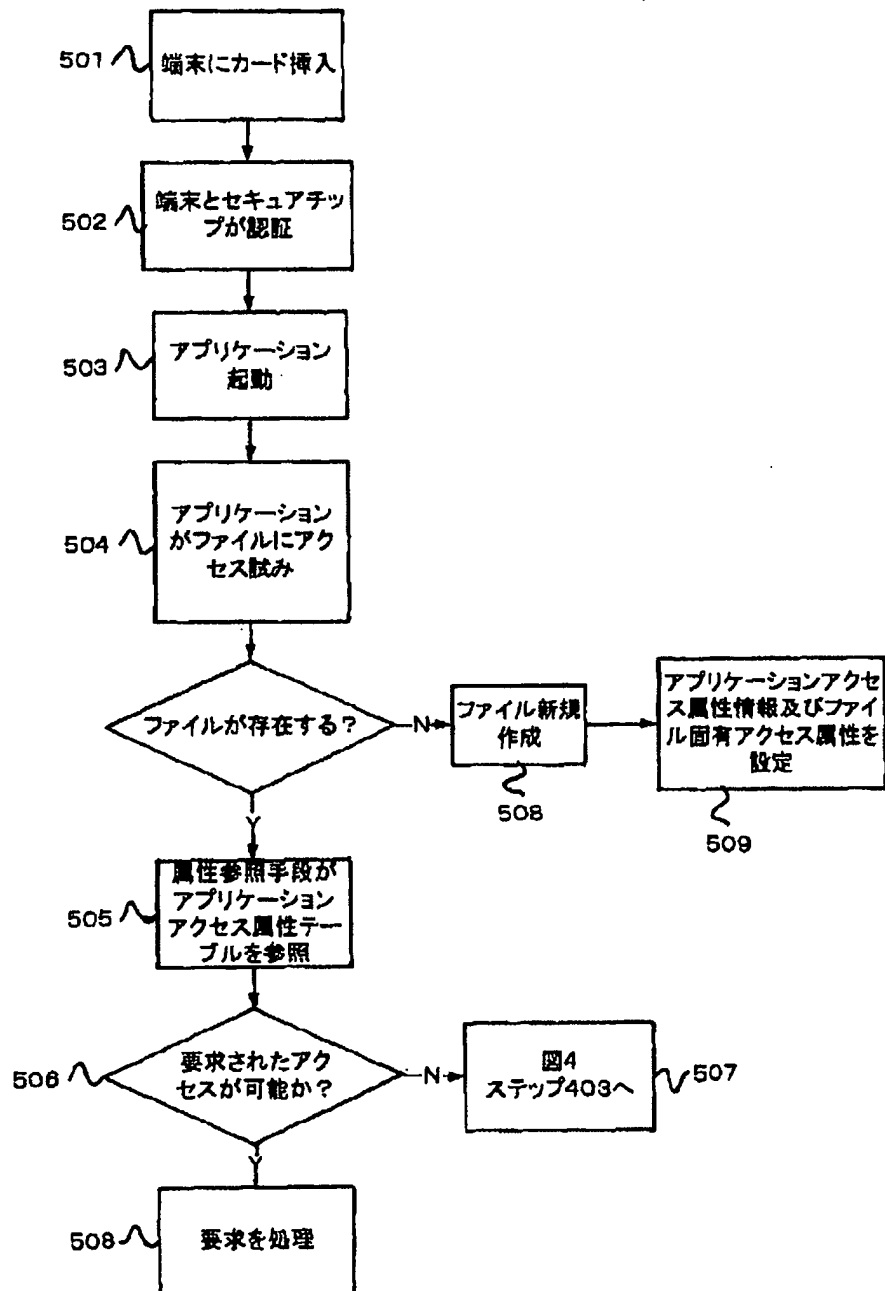
【図3】



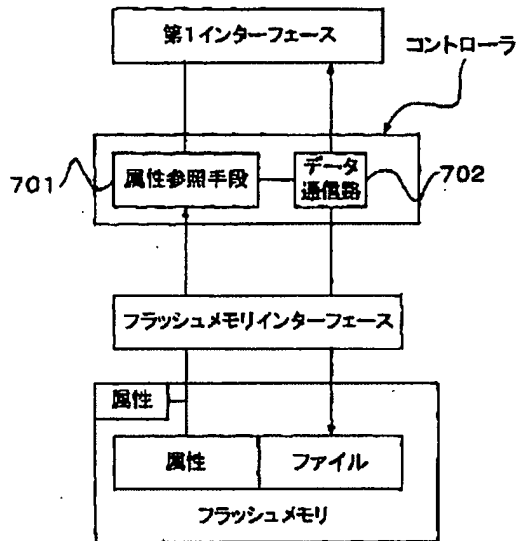
【図4】



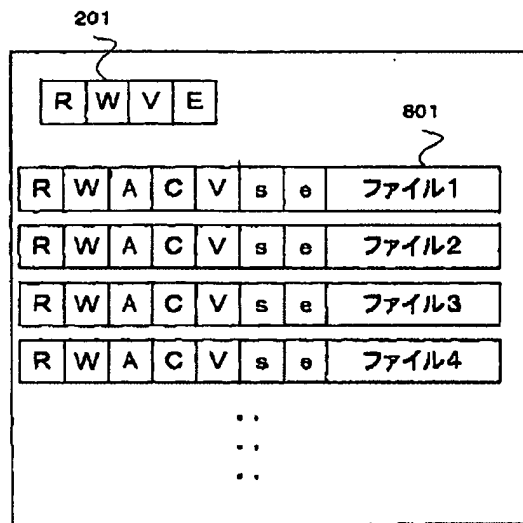
【図5】



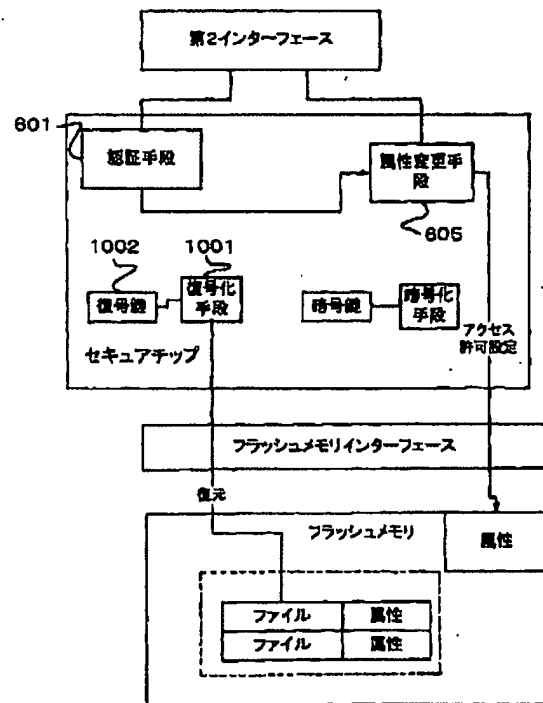
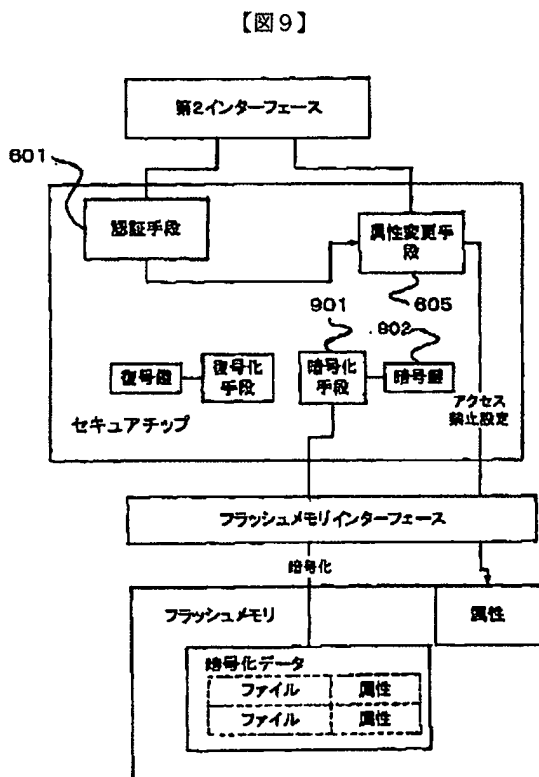
【図7】



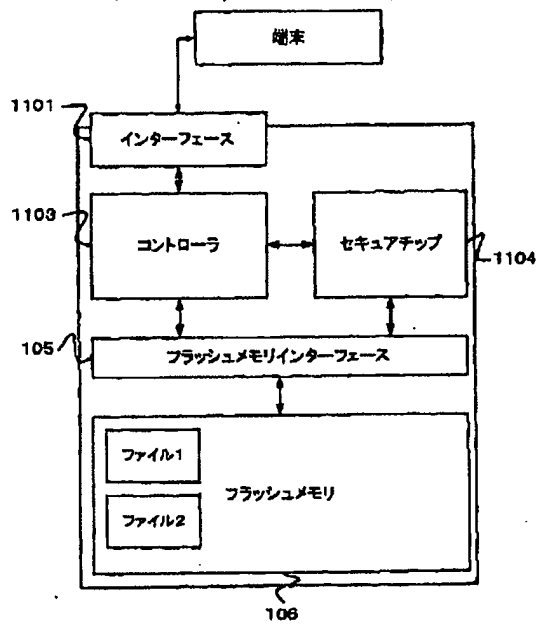
【図8】



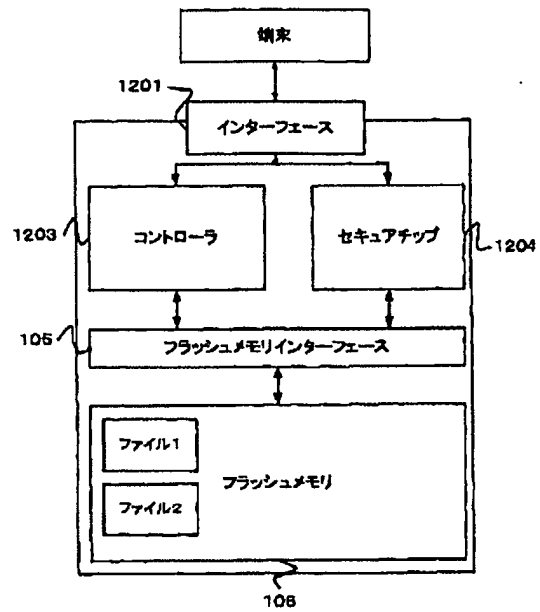
【図10】



【図11】



【図12】



フロントページの続き

(72)発明者 佐々木 理
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) SB017 AA07 BA06 BB06 CA16
SB035 AA13 BB09 CA38
SB082 EA11 JA06